

Single Sign On (SSO)

Information on our SSO system.

- [General documentation on our SSO system](#)
- [How to configure Passkeys](#)
- [How to terminate all sessions for a user on Keycloak](#)
- [Adding your logo and other visual elements \(branding\)](#)
- [How to change your password on Keycloak](#)
- [How to setup 2FA on Keycloak](#)
- [How to create a user on Keycloak](#)

General documentation on our SSO system

Single Sign-On (SSO) is a technology that allows users to log in once and access multiple applications without the need to log in again. Keycloak is the SSO system offered by our company that provides managed hosting services. It simplifies the authentication process and enhances the user experience.

SSO with Keycloak - features

At Cloud68.co we use [Keycloak](#), an well established open source platform, for user authentication. This is very helpful when you have more than one instance with us. Below are the main features of our SSO solution with Keycloak:

- **Centralized Authentication:** Keycloak provides centralized authentication for the majority (but not all) of the applications and services listed [here](#). Once the user logs in to Keycloak, they can access all the applications and services without the need to log in again.
- **Multiple Authentication Methods:** Keycloak supports multiple authentication methods, including username and password, two-factor authentication, and SAML-based authentication.
- **User Provisioning:** Keycloak supports user provisioning, which allows users to be added, modified, or removed from one or all your instances managed with us. You can do this yourself or [open a support ticket](#) so that we handle it.
- **Role-Based Access Control:** Keycloak supports role-based access control, which allows access to be granted based on the user's role in the organization.

Benefits of using Keycloak for your SSO needs

- **Improved Security:** a higher level of security is achieved with this approach, as users only need to remember one set of login credentials, reducing the risk of weak passwords and password reuse.
- **Support two factor authentication (2fa) when it is not possible.** Example: BigBlueButton does not support 2FA, but this can be implemented through Keycloak.

- **Simplified User Experience:** our SSO system simplifies the user experience by providing a single login for all applications and services, reducing the need for users to remember multiple usernames and passwords.
- **Increased Productivity:** your team can increase productivity by reducing the time it takes for users to log in to multiple applications and services.

Getting SSO for your infrastructure

Our SSO solution is available free of charge for all users that have at least three (3) managed hosting software (instances) on an active billing cycle. If you need less than three instances, the cost for the Managed Hosting Keycloak instance is 9Eur/month.

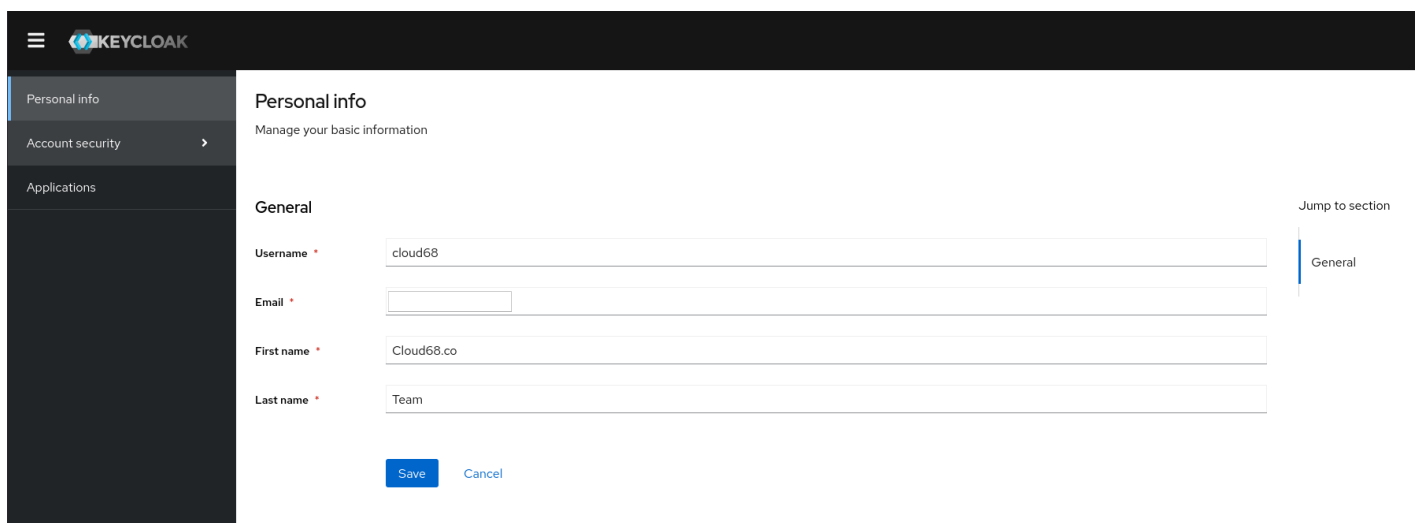
Keep in mind that not all platforms available on our website from [this page](#) support Keycloak and/or SSO for authentication.

How to configure Passkeys

Below is a step-by-step guide how to configure passkeys as an authentication method for Keycloak.

First step is to go to your **Keycloak URL** instance and login using your SSO credentials.

Upon login, you will land on the **Keycloak Console**.



The screenshot shows the Keycloak console interface. On the left is a dark sidebar with a menu containing 'Personal info', 'Account security', and 'Applications'. The main content area is titled 'Personal info' with the subtitle 'Manage your basic information'. Under the 'General' section, there are four input fields: 'Username' (containing 'cloud68'), 'Email' (empty), 'First name' (containing 'Cloud68.co'), and 'Last name' (containing 'Team'). Below these fields are 'Save' and 'Cancel' buttons. On the right side of the form, there is a 'Jump to section' link with 'General' selected.

Once there you need to go to **Account Security** and click **Signing in** which will open the authentication options.

Signing in

Configure ways to sign in.

Basic authentication

Password

Sign in by entering your password.

My password

Created October 17, 2025 at 12:11 PM.

[Update](#)

Two-factor authentication

Authenticator application

[Set up Authenticator application](#)

Enter a verification code from authenticator application.

Authenticator application is not set up.

Passkey

[Set up Passkey](#)

Use your Passkey to sign in.

Passkey is not set up.

Passwordless

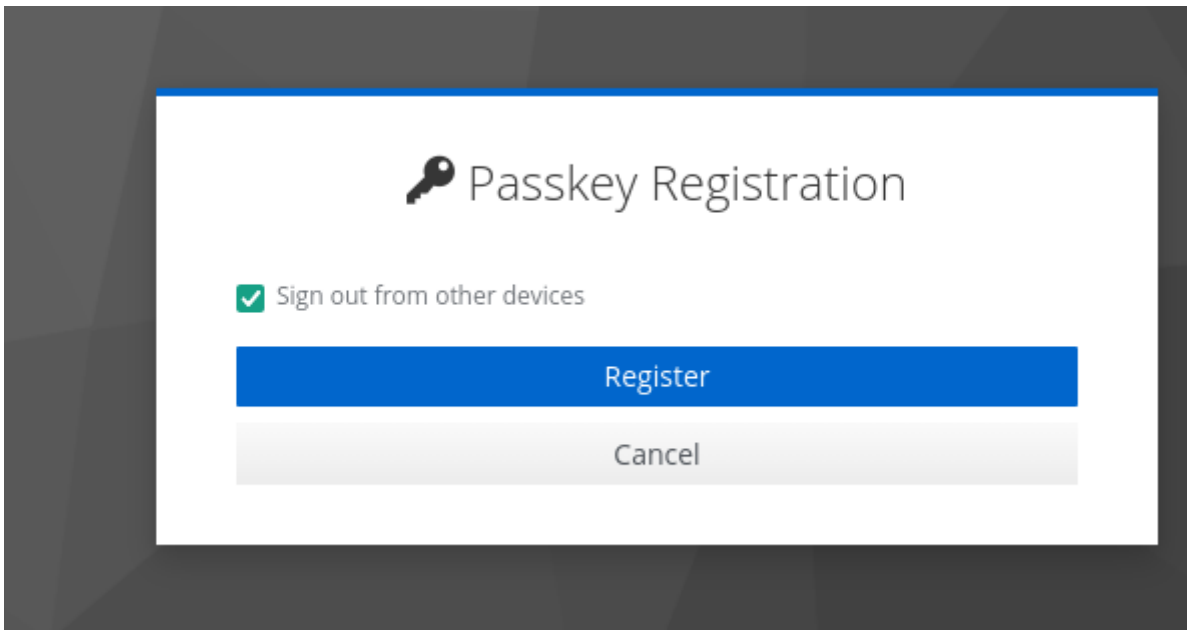
Passkey

[Set up Passkey](#)

Use your Passkey for passwordless sign in.

Passkey is not set up.

Click on **Set up Passkey**, and it will take you to a window to register the passkey as seen below.

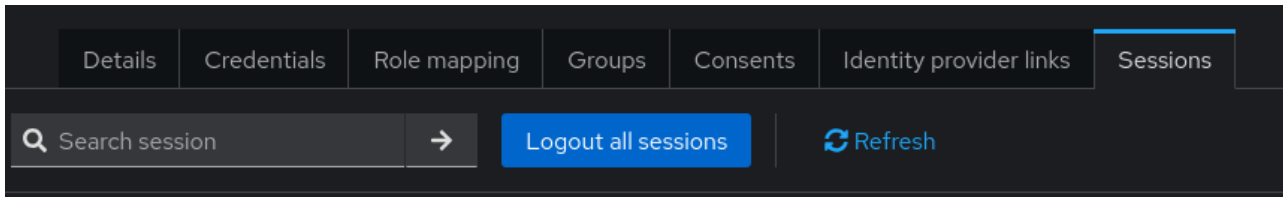


Follow the steps and configure your passkey, and you will be able to log in using your Titan keys.

There is also a way for users to enforce this way of authenticating and when the user logs in, it is required to set it up following the steps above, but this is only if all Keycloak users will use this method of authentication.

How to terminate all sessions for a user on Keycloak

1. Login to Keycloak and go to Users on the left panel.
2. Locate the user and click on the name to open their options.
3. Go to Sessions, last button on the panel and Logout all sessions.



Adding your logo and other visual elements (branding)

Unfortunately, you cannot make branding or visual customisations to your Keycloak instance directly. Changes such as uploading a logo, adjusting colours, or modifying other visual elements require modifications at the theme level, which fall outside the scope of what is accessible under our current Keycloak Managed Hosting setup and workflows.

To have these changes applied, you will need to open a support ticket as described in our [Tech Support \(FAQs\)](#) documentation.

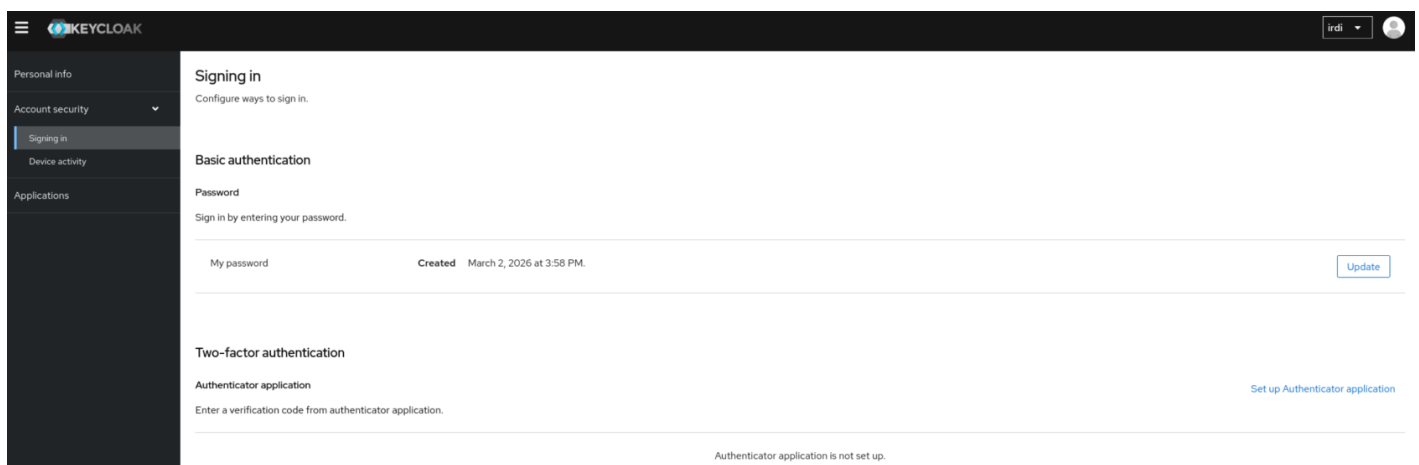
This service is provided free of charge for all subscribers who are receiving our [Add-On services](#).

How to change your password on Keycloak

Go to your Keycloak Console and Log in with your credentials.

Once logged in, go under Account Security → Signing in.

Under Basic authentication you will see and Update button next to My Password.



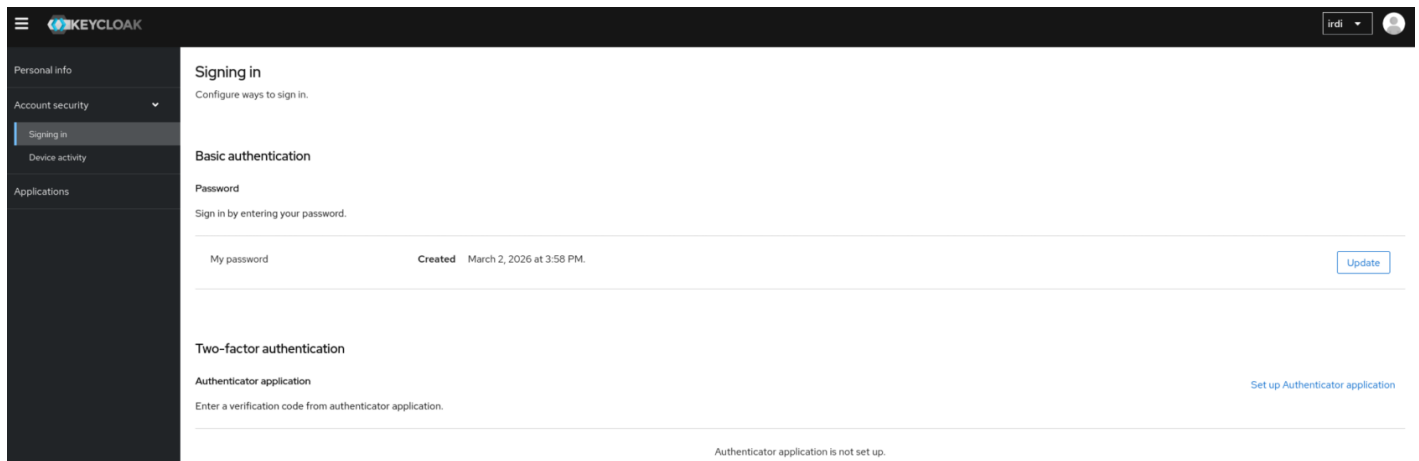
In case you do not know your Keycloak Login URL, please reach out to our [Support Team](#).

How to setup 2FA on Keycloak

Go to your Keycloak Console and Log in with your credentials.

Once logged in, go under Account Security → Signing in.

Under Two-Factor authentication click on Set up Authenticator application and follow the steps.



In case you do not know your Keycloak Login URL, please reach out to our [Support Team](#).

How to create a user on Keycloak

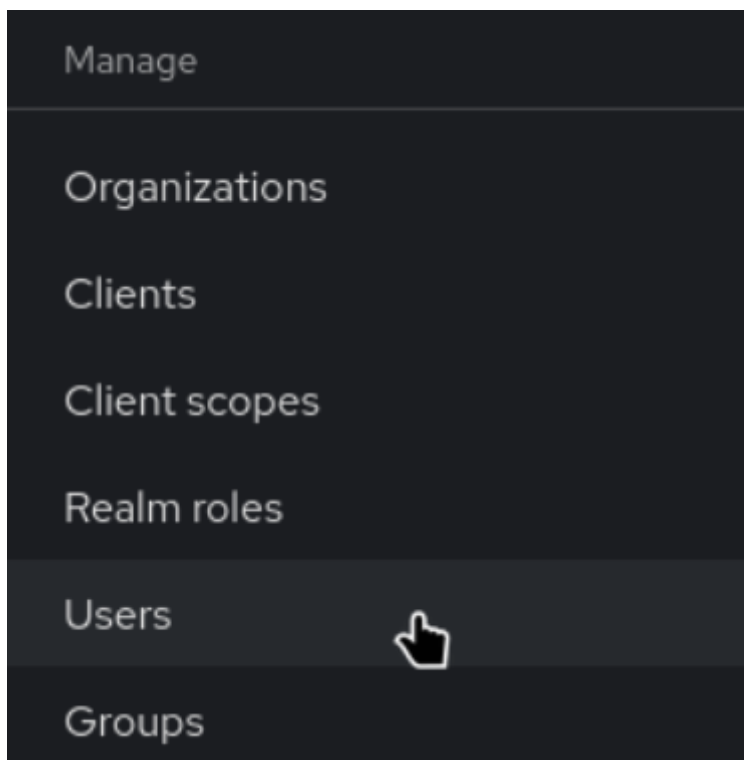
In order to create a new user on Keycloak follow the steps below.

1. Visit Admin Dashboard:

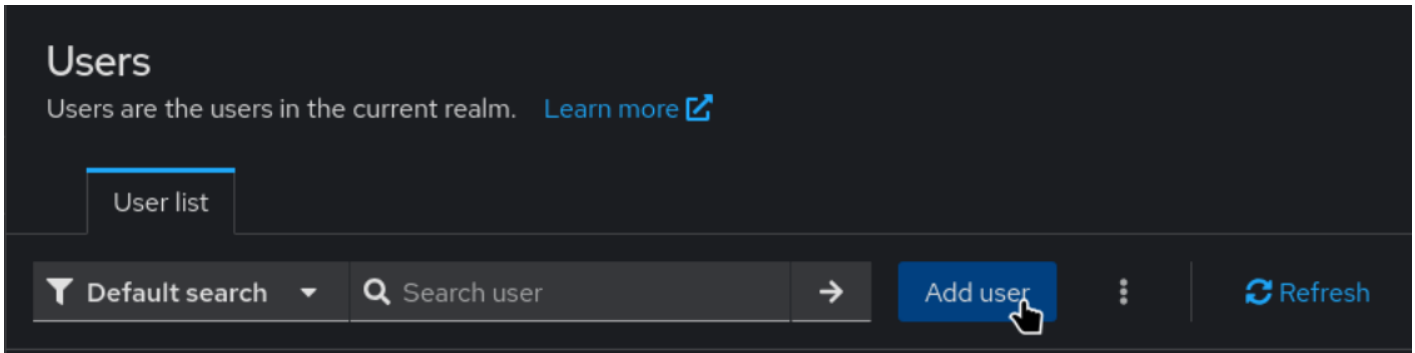
- Go to: Your Keycloak URL
- Log in using the admin account.

2. Create a New User:

- Navigate to **Users** on the left side of the dashboard.

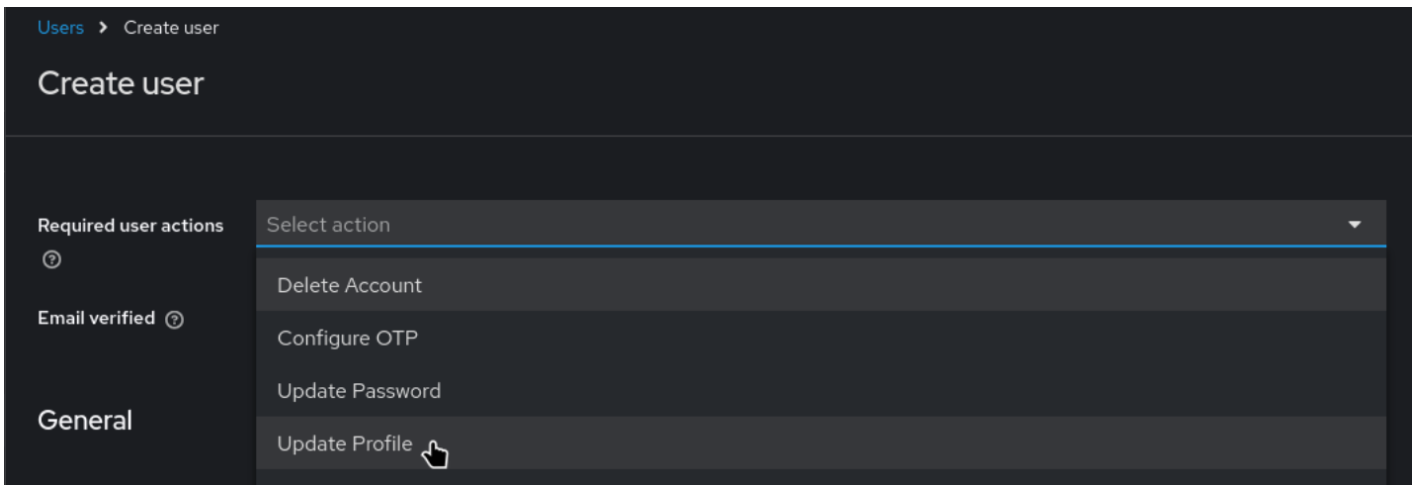


- Click on **Add User**.



- Under **Required user actions**, select **Update Profile**.

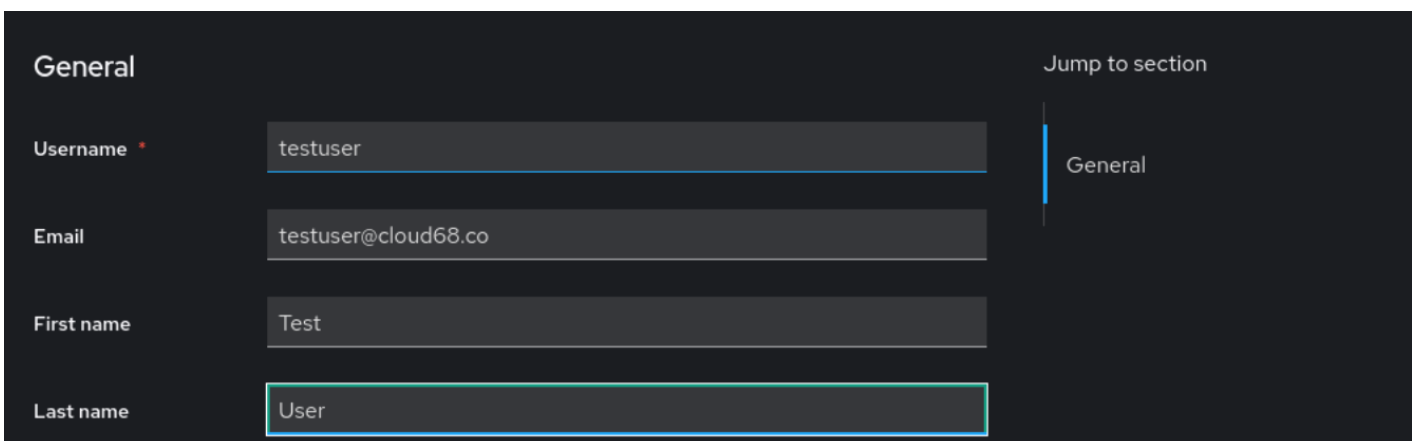
In case user impersonation is required leave this empty.



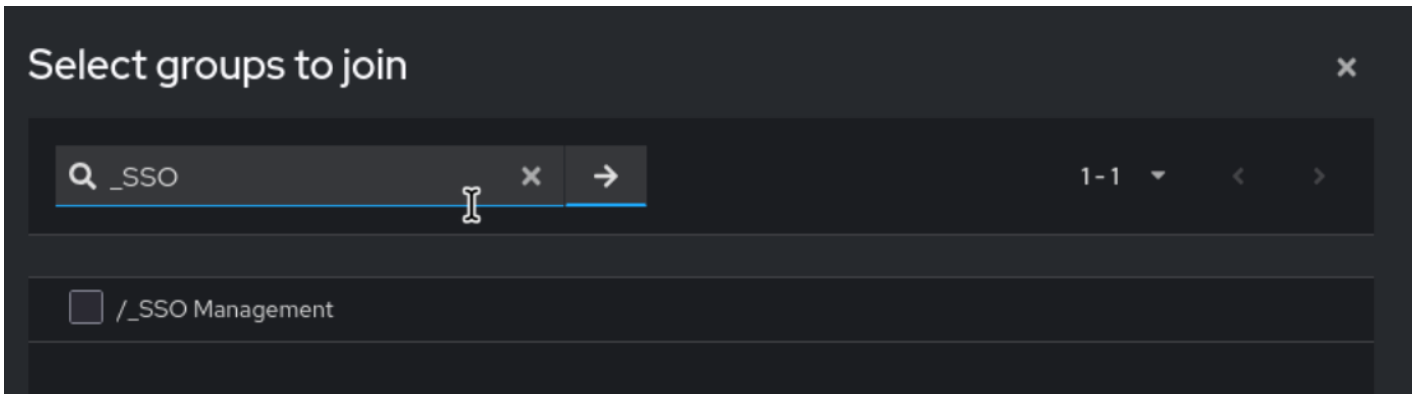
- Set **Email Verified** to **ON**.



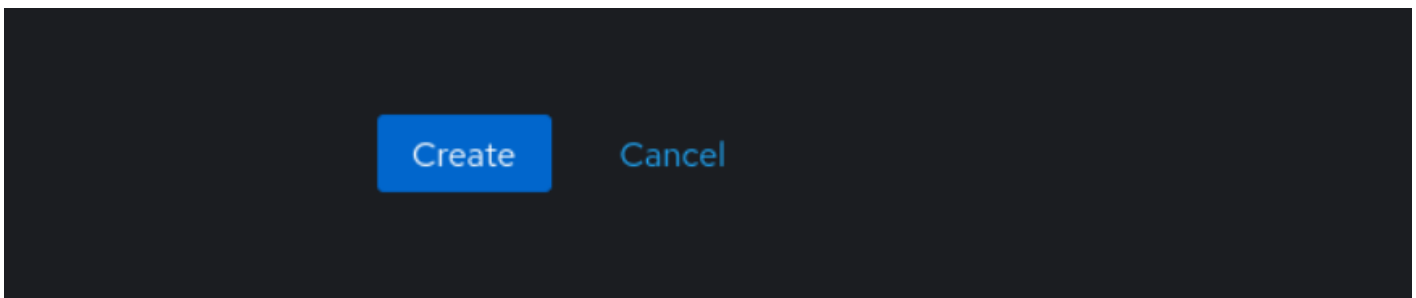
- Fill in the **Username**, **Email**, **First Name**



- Click **Join Groups** and add the user to the group it belongs.

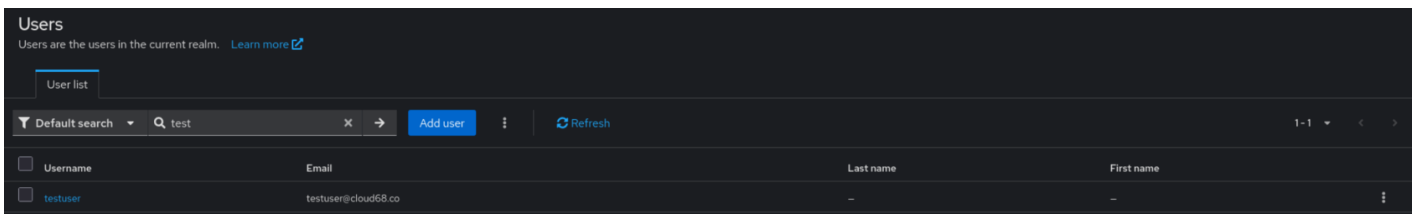


- Click **Create**

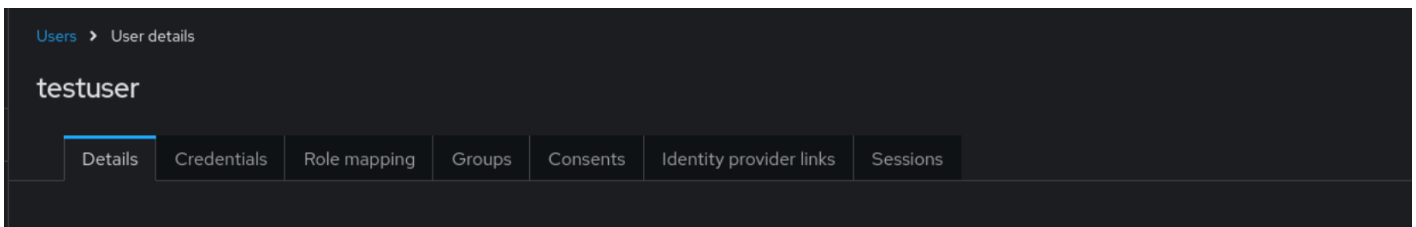


3. Send Password Reset Request:

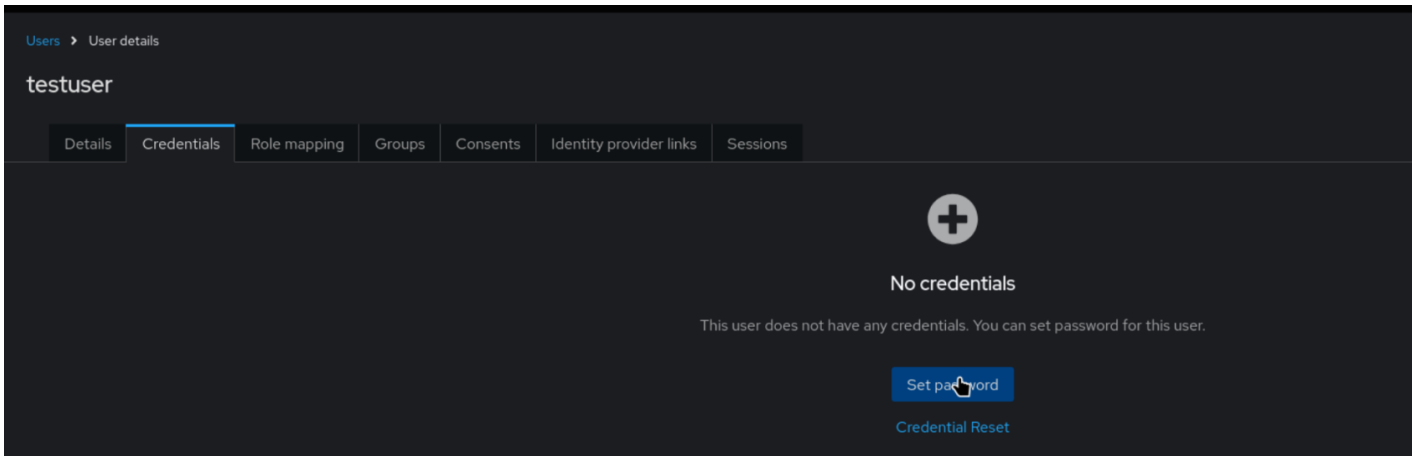
- Go to **Users**.



- Click on the newly created user.

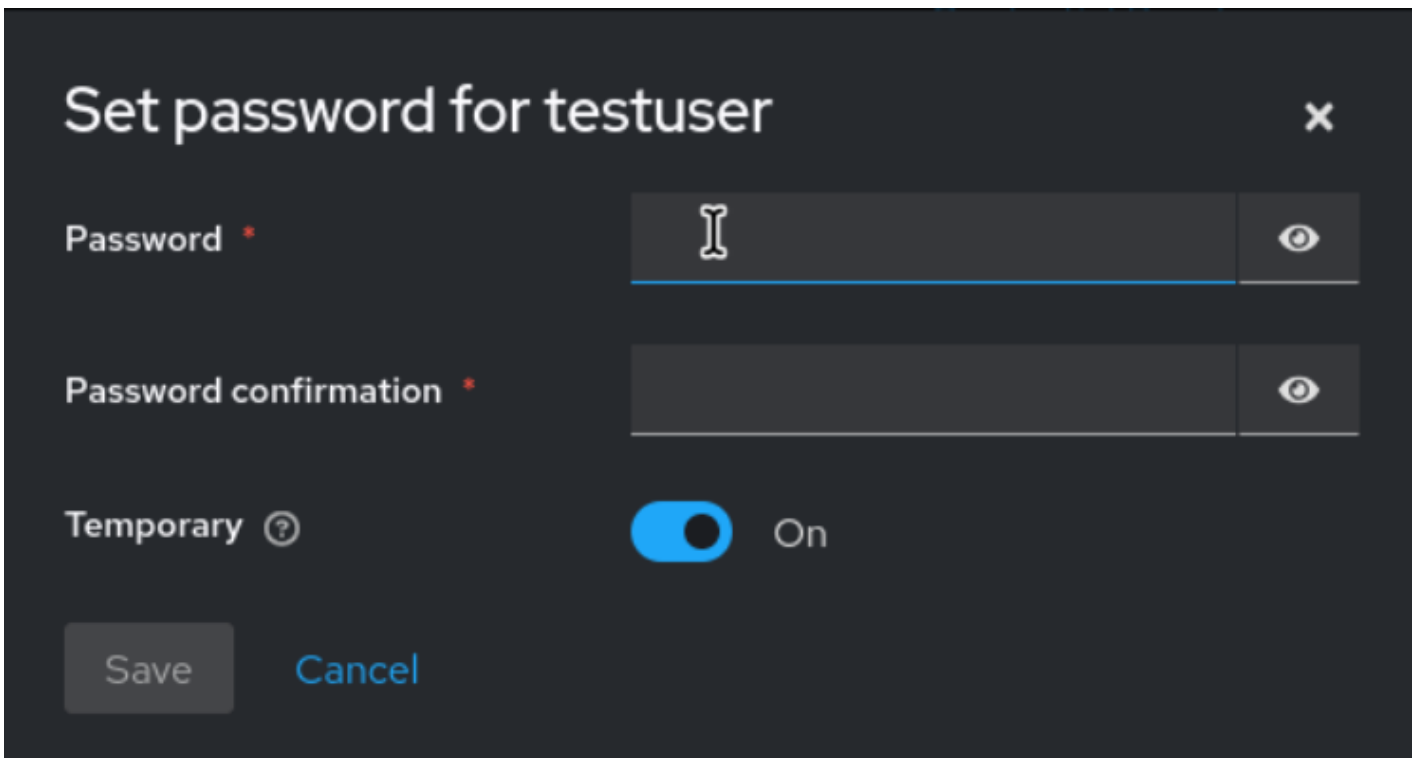


- Navigate to **Credentials** and click **Set a Password**.

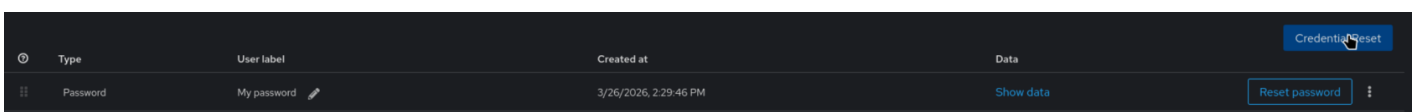


- Set a random Password and click **Save**.

In case user impersonation is required toggle "Temporary" to Off so it does not require setting up a password when impersonating.

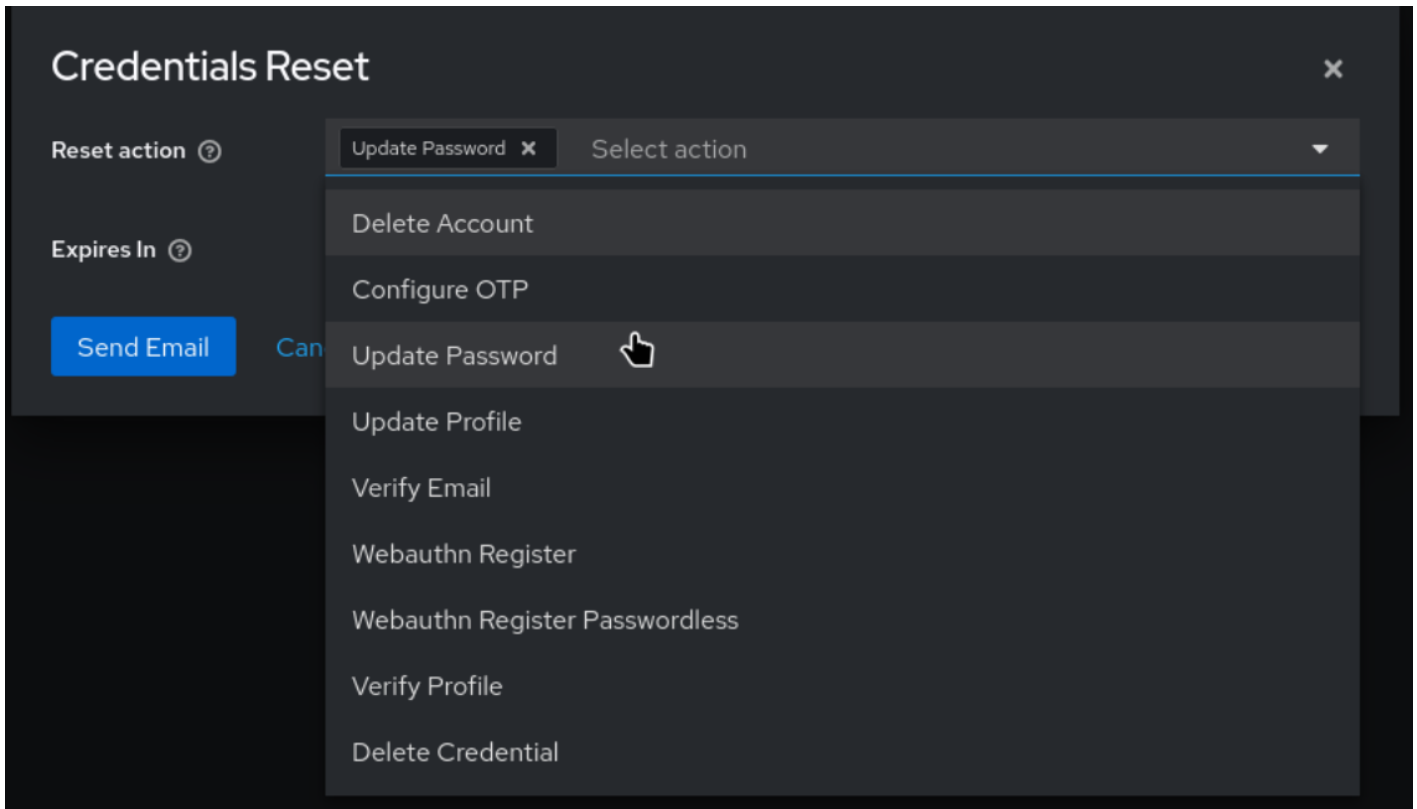


- Click **Credentials Reset**.

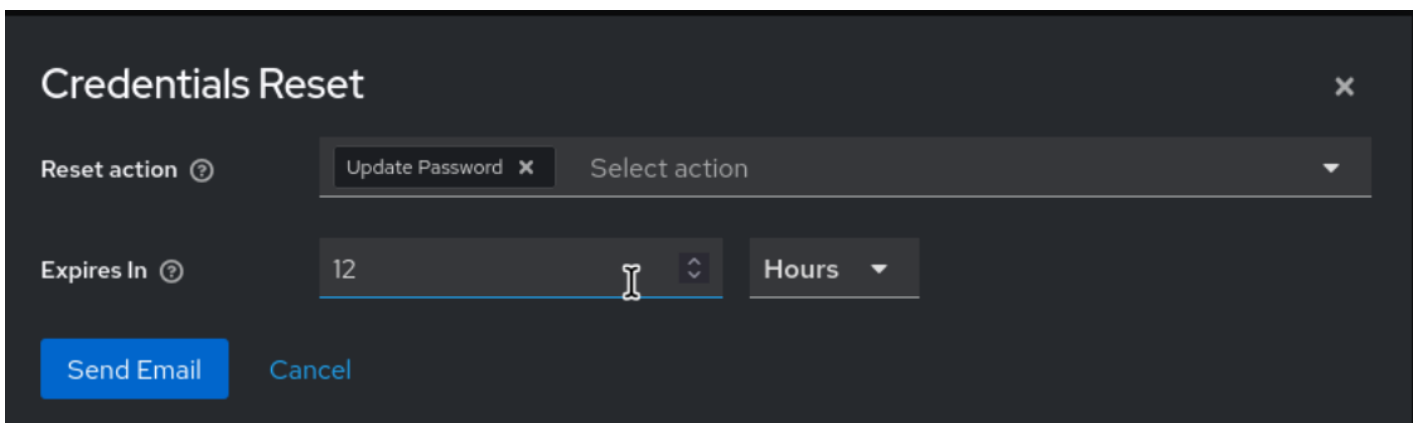


- On Reset action choose **Update Password**.

In case you followed the user impersonation steps, on this step choose Update password and Update Profile



- Choose an expiration time for the reset request and click Send.



- Notify the user that they now have an account and will receive an email to reset their password and update their profile.

In case you do not know your Keycloak URL reach out to our [support team](#).